MARÍA ALEJANDRA PROVÍTOLA
JUEZA

REDACTADO R. GHERCI
SECRETARIO

///en la ciudad de Buenos Aires, a los trece días del mes de agosto del año dos mil diecinueve, comparece ante S.Sa. y Secretario autorizante una persona, a la que se le hace saber que se le recibirá **declaración testimonial.** Previamente se le recibe juramento de decir verdad que presta en legal forma, y se le hacen saber las penas con que la ley reprime a quienes se pronuncian con falsedad y los derechos que le acuerdan los artículos 79 y siguientes, 242, 243 y 244 del C.P.P.N. Interrogado que es sobre sus condiciones personales, dice ser y llamarse: ***Claudio Ricardo Ramos,*** quien acredita identidad con D.N.I. N° [redacted] que exhibe y retiene para sí, de nacionalidad argentino, de estado civil casado, Subcomisario de la División Investigaciones de Delitos Tecnológicos de la Policía Federal Argentina, con domicilio Cavia 3602, piso 1° de esta ciudad, teléfono 4800-1120.----------

Se deja constancia que en el presente acto se encuentra presentes el Subcomisario Carlos Alberto Aguirre –Jefe de la División Investigaciones de Delitos Tecnológicos de la Policía Federal - y el Comisario Ricardo Rubén Rochas –jede del Departamento de Ciber Delito de la Policía Federal-.----------

Preguntado para que diga si posee vínculos de parentesco y/o interés con las partes, responde que no y que será veraz en sus dichos. Invitado Ramos por S.Sa. a manifestar cuanto conozca sobre el hecho que se investiga, **DECLARA:** Que comparece a los fines de denunciar que el día 29 de julio de 2019, a eso de las 13:00 horas, tomé conocimiento por parte de la Superintendencia de Bienestar de la Policía Federal, que ese mismo día, en horas de la mañana, se recibieron en varias dependencias de la Policía Federal, del Área de Drogas, un correo electrónico que simulaba provenir de la Superintendencia de Bienestar, el cual contenía un link, el cual al ser accionado por cualquier funcionario de cualquier dependencia policial, rediccionaría a un formulario el cual

#33913287#241391080#20190813123617313

solicitaba se completen datos personales e inclusive datos de usuarios y contraseñas de cada afiliado. Esta maniobra es conocida como “Phishing”. Concretamente se detectó inicialmente que se recibió un correo desde la Dirección de correo electrónico div.supbienestar@hotmail.com. Que ese correo fue inicialmente receptado en la casilla oficial acti_drogas@policíafederal.gov.ar, de la Superintendencia de Drogas Peligrosas de la Policía Federal, que al notar extraño que el emisor del correo tuviera como servidor al Hotmail, alertó a la superioridad y no habrían ingresado al link en cuestión. Pr lo que en ese caso no se habría concretado la sustracción de datos. Que se corroboró que dicho correo no pertenece a la institución. Sin embargo se desconoce con exactitud a cuantas dependencias oficiales fue remitido el correo engañoso. Posteriormente se detectó también que el mismo correo se receptó también en las Áreas de Despacho y Logística de la oficina de Drogas de Policía Federal de la Provincia de Tucumán. Los correos electrónicos donde se recibieron estos correos, es decir los “mails comprometidos” como se mencionan en el estudio que en este acto adjunta son divantidrogastucuman@gmail.com,areaoctava.mesopotamia@gmail.com y divpersonalsuperior@gmail.com, casillas oficiales asignadas a diferentes áreas la Superintendencia de Drogas de la Policía Federal. Que a partir de ello, personal técnico de la dependencia a su cargo logró a partir del análisis de uno de los correos electrónicos comprometidos divantidrogastucuman@gmail.com, logró determinar que en el mismo existieron distintos tipo de “alertas” por accesos que fueron registrados por Gmail los cuales quedaron en la papelera de reciclaje del mismo correo. Es decir, que en ese correo ingresaron mails emitidos por la empresa Gmail donde se alerta que ese correo electrónico estaba siendo abierto desde otra computadora distinta a la utilizada habitualmente por

#33913287#241391080#20190813123617313

el agente oficial. De las propiedades técnicas de esa alerta se pudieron determinar dos IPs que se corresponderían con las conexiones utilizadas por la persona que habría obtenido los datos de forma engañosa e ingresó a la cuenta oficial sin autorización. Se trataría de las IP 199.58. usada el 29 de julio de 2019 a las 0.42 hs. y 45.232. usada el 29 de julio de 2019 a las 0.39 hs. Dichas IP fueron asignadas por la empresa Fulltech solutions SH de la provincia de Entre Ríos, desconociéndose por el momento a que usuario en particular fueron asignadas. Que del análisis efectuado al correo areaoctava.mesopotamia@gmail.com y mediante la misma maniobra antes descripta se detectaron ingresos no autorizados desde las IPs 199.58. el 29 de julio de 2019 a las 00.42 hs y 45.232. el mismo día a las 00.39 hs., ambas también asignadas por la empresa Fulltech solutions SH de la provincia de Entre Ríos. Que a través del Ministerio de Seguridad de la Nación, en el día de ayer, en horas de la mañana se enteró que en la red social Twiter un usuario: "@lagorraleaks2.0" había hecho mención que había subido a la "Deep web" información relacionada con la Policía Federal, específicamente de las áreas de bienestar y drogas peligrosas, razón por la cual supone que la información allí publicada puede ser la obtenida a través del mecanismo antes descripto. Que el usuario en cuestión se regodeaba de haber subido información confidencial de la policía federal e incluso información personal de sus integrantes. Que respecto de la "Deep web" refiere que se trata de un área de internet sin control por parte de las empresas internacionalmente conocidas como por ejemplo Google y donde resulta muy difícil rastrear a los usuarios e información que allí se vuelca. Por otra parte hace saber que teniendo en cuenta la modalidad y tipografía utilizadas por el usuario de Twiter "@lagorraleaks2.0" se lo puede relacionar con las personas que en el año 2017 hackearon la cuenta de la Ministra Patricia

Bullrich, llamados R D M M que utilizada cono usuario “N o ” y E V S , más aún cuando el propio usuario “@lagorraleaks2.0” hizo mención en este último episodio por la red social Twiter que precisamente ahora volcaría la información de la Policía Federal de la misma forma en la que en el año 2017 había hecho respecto de la Ministra. Que según cree por aquel hakeo los nombrados fueron oportunamente condenados. Aclara que en la actualidad se tomaron medidas para la preservación de las conexiones institucionales que por ello no corren riesgo. Que sugiere como medida para poder dar con los autores del hecho, que el juzgado libre orden de presentación a la empresa proveedora de internet Fulltech solutions SH de la provincia de Entre Ríos a efectos de que se informe al momento de la presentación a que usuario se asignaron las IP referidas. También solicitar a la firma Hotmail información de la cuenta en cuestión. Aporta asimismo, impresiones de pantalla de la red social Twiter a las que hiciera mención que se agregan por orden de S.S..Es todo cuanto puede aportar al Tribunal, por lo que no siendo para más, se da por finalizado el acto, previa lectura efectuada en alta voz por el Actuario y ratificación hecha por el compareciente para sí, firmando de conformidad, luego de hacerlo V.S. por ante mí, de lo que DOY FE.

MARÍA ALEJANDRA [illegible]
JUEZA

[illegible]
SECRETARIO

#33913287#241391080#20190813123617313